DETAILED ACTION

1. This action is in response to application filed May 19, 2005. Claims (22-42) are pending.

Priority

2. Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) - (d) is acknowledged.

The application is filed on May 19, 2005 but is a 371 case of PCT/DE03/03853 application filed 11/20/2003 and has a foreign priority application filed on 12/17/2002.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 22-29 and 31-42 are rejected under 35 U.S.C. 102(b) as being anticipated by Davis (European Patent Application 0784256 (cited from IDS)).

4. As to claim 22, Davis teaches a **method for operating a security module, said method comprising the steps of:**

providing a security module having a secure key memory and at least one data interface [43, 44, fig. 5];

in a personalization state, setting up a connection to a personalization unit using the data interface [21, 44, fig. 5];

using the security module to create a module key pair afresh and storing said module key pair in the key memory [abstract; lines 5-9];

sending a public module key to the personalization unit via the connection (i.e., … teaches output public key [col. 7, lines 18-22]);

using the personalization unit to produce a certificate relevant to the public module key by signing with a signing key from the personalization unit (i.e., … teaches digital signing [col. 7, lines 34-38]);

causing the personalization unit to send the certificate to the security module and storing said certificate securely therein (i.e., … teaches certificate is input to hardware agent and stored [col. 7, lines 34-38]);

clearing down the connection between the security module and the personalization unit (i.e., … teaches connection verification [col. 7, lines 40- 45]);

changing the security module from a personalization state to an operating state;

and setting up in the operating state (i.e., processor for procession operations [col. 4, lines 9-11])**, a cryptographically secure connection to a central system** (i.e., … teaches encrypted communication in [col. 7, lines 55-59; col. 7, lines 1-5])**, said connection involving the use of a private module key and involving the public module key together with the certificate being transmitted to the central system,**

where the certificate is checked (i.e., ... teaches hardware agent verification using certificate through encrypted communication [col. 8, lines 32-38]).

5. As to claim 23, Davis teaches a **method where changeover to the personalization state erases** (i.e., update) **the module key** (i.e., … teaches the prior generated public key is updated with new unique public key [col. 7, lines 20-30].

6. As to claim 24, Davis teaches a **method where in the personalization state the connection between the security module and the personalization unit is checked cryptographically for authenticity and is protected against corruption** (i.e., ... teaches generating a challenge value to be verified [col. 7, lines 51-59; col. 8, lines 1-17]).

7. As to claim 25, Davis teaches a **method where a public key from the central system is transmitted together with the module certificate** (i.e., … teaches a decrypting the certificate to obtain the public key [col. 7, lines 45-53]), **said public key being used in the operating state to check the authenticity of the central system** (i.e., … teaches public key used in authentication [col. 7, lines 17-40])

8. As to claim 26, Davis teaches a **method where the public key from the central system is signed with the signing key from the personalization unit** (i.e., … teaches public key sign with private key [col. 7, lines 30-35]), **and the**

resultant certificate is also transmitted and is checked by the security module (i.e., … teaches a certificate is use for authentication [col. 7, lines 30-40]).

9. As to claim 27, Davis teaches a **method where a signer's public signing key is signed by the central system creating another certificate** (i.e., … teaches public key sign with private key [col. 7, lines 30-35]), **and this certificate is also transmitted and is checked by the security module** (i.e., … teaches a certificate is use for authentication [col. 7, lines 30-40]).

10. As to claim 28, Davis teaches a **method where the key memory in the security module stores a public checking key from a manufacturer** (col. 5, lines 1-10), **the personalization unit transmits its public signing key together with a certificate** (i.e., … teaches decrypting certificate to obtain key [col. 7, lines 45-50], **formed with the checking key from the manufacturer, and the security module first checks the public signing key's certificate with the public checking key and then checks the certificates produced with the public signing key, and changes to the operating state only if the check is successful** (col. 8, lines 40-59).

11. As to claim 29, Davis teaches a **method where the security module is used to form a permanent identity key on a one-off basis** (i.e., … teaches permanently programs the key into memory [col. 7, lines 34-38], **the associated public key is signed with the checking key from a manufacturer** [col. 7, lines 30-35], **and the**

corresponding certificate is stored in the security module [col. 7, lines 35-40], **and wherein the identity key with a certificate is used to assure the personalization unit of authenticity on the basis of a challenge-response method** (i.e., ... teaches generating a challenge value to be verified [col. 7, lines 51-59; col. 8, lines 1-17]).

12. As to claim 31, Davis teaches a **method where the personalization system sends a variation value to the security module, which is used when the new module key is produced** [col. 7, lines 17-27].

13. As to claim 32, Davis further teaches a **method where the connection** (i.e., encrypted communication) **to the central system which has been set up using the private module key is used to interchange a symmetrical key for subsequent transaction connections and to store it in the secure key memory in the security module** (i.e., … teaches encrypted communication connection for which an encryption operation was performed with a private key [col. 7, lines 55-59] Davis teaching a decryption operation performed using public key for which was obtained and stored from a previous certificate [col. 8, lines 1-5]).

14. As to claim 33, Davis teaches a **method where a mobile personalization unit is used which is connected to the security module directly via a connection which is controlled by a user** [fig. 5].

15. As to claim 34, Davis teaches a **method where a user inputs a one-off transaction number** (i.e., challenge value) **into the security module, either directly using an input unit which is connected permanently to the security module or immediately and directly using an input unit which is connected to the security module by the user, and the connection to the personalization unit is protected by transmitting the transaction number** (i.e., ... teaches generating a challenge value to be verified [col. 7, lines 51-59; col. 8, lines 1-17]).

16. As to claim 35, Davis teaches a **method where a mobile appliance is connected to the personalization unit via a local connection** (i.e., electrical connection) **to the security module, which local connection is controlled directly by a user, and a long-distance connection, the mobile appliance identifies** (i.e., certification) **itself to the personalization unit, and as a result the security module is indirectly identified to the personalization unit** (col. 7, lines 3-6).

17. As to claim 36, Davis teaches a **method where the local and long-distance** (i.e., remote) **connections are used merely for securely setting up a secure direct network connection between the security module and the personalization unit** (i.e., … teaches remote communication [col. 7, lines 40-50]).

18. As to claim 37, Davis teaches a **method for personalizing a security module, comprising the following steps:**

connecting a security module to a personalization unit (fig. 4);

connecting the security module temporarily to an identification unit the connection (i.e., electrical connection) **being accomplished by a user using an interface which is determined by the user** (col. 7, lines 3-6);

sending (i.e., transmit) **via the identification unit, an identification value** (i.e., challenge value) , **which can be checked by the personalization unit, to the security module, which forwards it to the personalization unit** (i.e., … teaches a challenge value transmitted [col. 8, lines 55-59]);

and where the personalization unit performs the personalization if the check on the identity value is positive (i.e., … teaches positive comparison check using challenge value [col. 9, lines 1-10]).

19. As to claim 38, Davis teaches a **method where the identification value** (i.e., challenge value) **is a one-off transaction number** [col. 9, lines 1-10].

20. As to claim 39, Davis teaches a **method where the identification value** (i.e., challenge value) **is interchanged between the identification unit and the personalization unit using a cryptographically authenticated data connection** [col. 7, lines 50-59].

21. As to claim 40, Davis teaches a **security module comprising:**

a programmable processor including memory for storing a secure key [fig. 5];

at least one data interface for releasably coupling said security module to a personalization unit [21, 44, fig. 5];

means for creating a module key pair storable in said memory and for sending said module key to said personalization unit [col. 7, lines 17-26];

means for receiving and securely storing a certificate sent from said personalization unit [col. 7, lines 34-40];

operating means (i.e., supplying power) **for changing said security module from a personalization state to an operating state once said security module is no longer coupled to said personalization unit** (i.e., … teaches hardware place on a system for which establishes a electrical connection [col. 7, lines 1-7] One of ordinary skill in the art would recognized the statement of "place on for which establishes a electrical connection" inherently teaches the ability to de-couple the hardware from the system);

and means for establishing a cryptographically secure connection to a central system using a private module key, said public module key and said certificate (col. 7, lines 55-59; col. 8, lines 1-5).

22. As to claim 41, Davis teaches a **personalization unit comprising:**

at least one data interface for coupling (i.e., electrical connection) **said personalization unit to a security module** [col. 7, lines 1-9];

means for receiving a module key via said interface, said module keying being sent from said security module [col. 7, lines 9-17];

means for generating a signing key and producing a certificate regarding said module key, said certificate being produced by signing said module key with said signing key [col. 7, lines 30-35];

and means for sending (i.e., output) **said certificate to said security module** (col. 7, lines 45-50) .

23. As to claim 42, Davis teaches a **central system comprising:**

a secure key memory [col. 7, lines 40-50 and lines 34-38];

at least one data interface [21, fig. 4];

means for receiving a private module key [21, fig. 4];

a public module key and a certificate from a security module [col. 7, lines 34-38];

means for establishing a cryptographically secure connection to said security module using said public module key, said private module key and said certificate (col. 7, lines 55-59; col. 7, lines 1-5)**;**

and means for checking said certificate (i.e., ... teaches comparing key from decrypted certificate to determined keys are identical [col. 8, lines 50-55] … if the key are different therefore certificate check fails and communication is terminated).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

24. Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis in view of Hind et al. (US Patent No. 6,826,690 and Hind hereinafter).

25. As to claim 30 the system disclosed by Davis shows substantial features of the claimed invention (discussed in the paragraph above), it fails to disclose:

A method where the security module sends the personalization module one of a time stamp and a random value which is included in the signature when the certificates are formed.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Davis as introduced by Hind. Hind discloses:

> **A method where the security module sends the personalization module one of a time stamp and a random value which is included in the signature when the certificates are formed** (to provide a certificate with a timestamp, random number and signature [fig. 5B]).

Therefore, given the teachings of Hind, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Davis by employing the well known features of a certificate containing a timestamp, random number and signature disclosed above by Hind, for which security will be enhanced [col. 3, lines 23-26].

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2131

/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2131